The Future of SET

Pita Jarupunphol and Chris J. Mitchell
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX
Tel. (44) 01784 414125, (44) 01784 443423
P.Jarupunphol@rhul.ac.uk, C.Mitchell@rhul.ac.uk

Abstract

According to Hassler (2000), the Secure Electronic Transaction (SET) scheme is one of a small number of industry standard means for securing Internet e-commerce communications. Although SET potentially offers a high level of security protection for e-commerce transactions, there have been a number of criticisms of SET, including of its complexity and cost of implementation. These problems have restricted SET implementation and use. However, SET has been continuously improved since it was first released in 1997, including the development of a number of SET extensions. This paper assesses how well SET meets merchant and consumer security requirements. In addition, this paper also analyses criticisms of SET and considers its future in Internet e-commerce security.

Keywords: Electronic commerce (E-commerce), Secure Sockets Layer (SSL), Secure Electronic Transaction (SET), Transport Layer Security (TLS), cryptography, digital certificates, digital signatures, digital wallets.

Word count: 3,867 words, 10 pages

1 INTRODUCTION

E-commerce is becoming an important means of doing business for many organisations. In addition, it also provides consumers with a convenient way of shopping. For example, consumers can make an order via the Internet, which can be much more convenient than conventional shopping, (Whiteley 2000). However, unlike other conventional shopping methods, there is no face-to-face contact in e-commerce, and significant security issues arise. Financial fraud is arguably an issue of particular concern to e-commerce consumers. Consumers are worried that their financial information will be compromised, (Caldwell 2000). Furthermore, a significant number of consumers are concerned about the trustworthiness of their merchants. As a consequence, it is important to have industry standard means for securing Internet e-commerce communications.

There are a small number of standardised means of providing e-commerce security for Internet e-commerce transactions. Of particular practical importance are Secure Sockets Layer (SSL) and IETF's SSL-based Transport Layer Security (TLS). SSL and TLS provide data transmission security between senders and receivers, (Oppliger 2000, Rescorla 2001) – see figure 1.

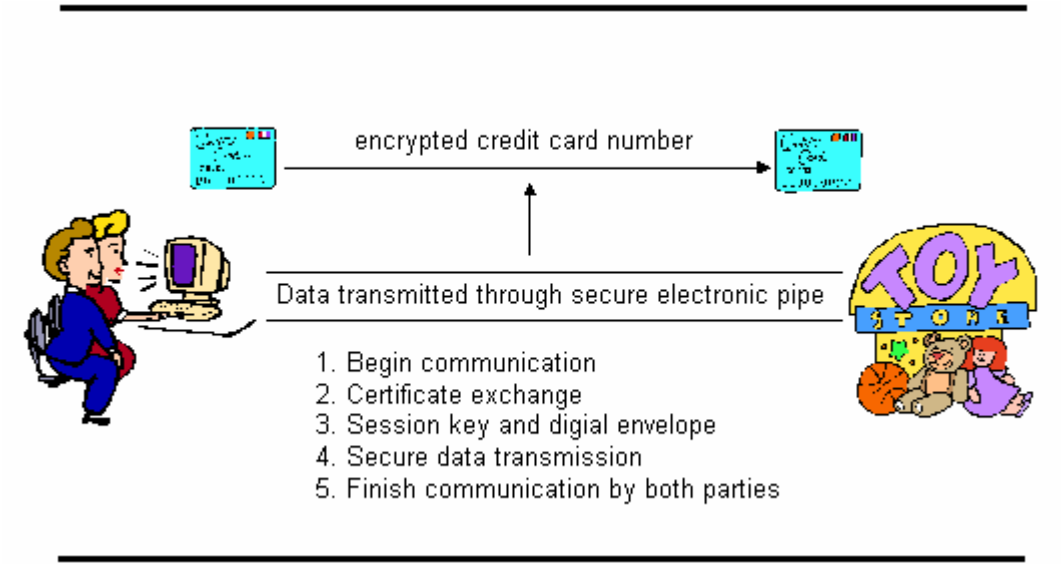

Figure 1. SSL process in e-commerce transactions.

An alternative approach is provided by SET, which has been established specifically for securing entire transactions (SET 1997a). Probably for pragmatic rather than security reasons, SSL is almost always used in preference to SET for Internet e-commerce security, and SET has not really taken off. Ease of installation and cost of investment are arguably the main problems restricting the adoption of SET. As a consequence, this paper will evaluate criticisms of SET, and assess the future of this industry standard for security.

2 THE ROLE OF SET IN E-COMMERCE

Since e-commerce allows people to place an order via the Internet, there are also several potential associated security threats. Online fraud is arguably an issue of concern to all e-commerce participants, including consumers, merchants, and their respective financial institutions. SET, which was invented by Visa (http://www.visa.com) and MasterCard (http://www.mastercard.com), is a method to secure entire e-commerce transactions. SET is arguably able to address several categories of fraud in Internet e-commerce transactions. The operation of SET can be explained as follows (also see figure 2), (SET 1997a, Stein 1998).

Stage 1. SET initialisation begins after the SET participants (consumer and merchant) have exchanged their identities.

Stage 2. The cardholder selects their purchases and submits an order and payment form to the merchant server. Consumer purchase information will be divided into 2 blocks: order information (OI) and payment information (PI). OI will be encrypted using the merchant public key, whereas PI will be encrypted using the acquirer public key. The consumer PC generates a digital signature on both OI and PI and sends the signatures along with the encrypted OI and PI.

Stage 3. The merchant receives the encrypted OI and forward encrypted PI to an acquirer via payment gateway for payment authorisation. The payment gateway can decline the transaction based on the information received from the merchant.

Stage 4. The acquirer requests payment authorisation from the issuer via the financial payment network.

Stage 5. The issuer responds to the payment request to the acquirer via the financial payment network. The acquirer then sends a payment authorisation to the merchant.

Stage 6. The merchant confirms the transaction after having received payment authorisation from the acquirer.

Stage 7. The merchant requests the acquirer to capture the transactions.

Stage 8. The issuer issues a bill to the cardholder at some time after confirmation of the transaction.

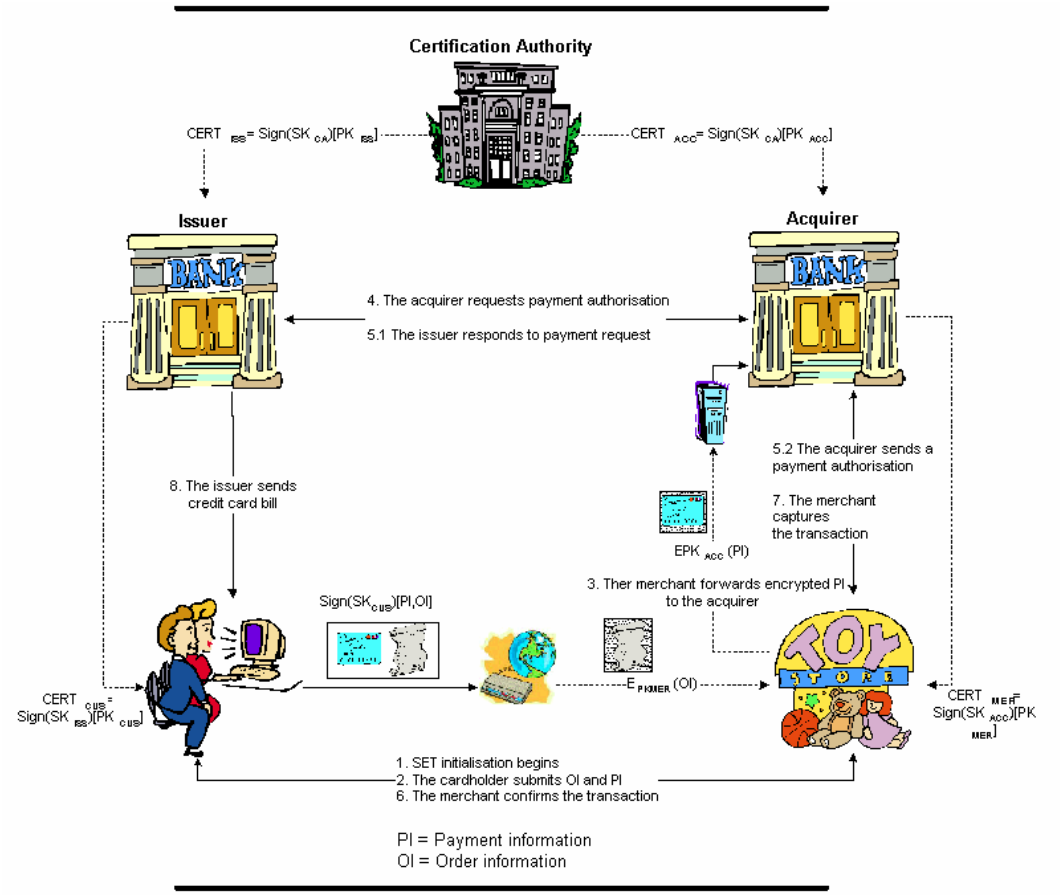

Figure 2. SET process in e-commerce transactions.

2.1 Credit card fraud

SET supports long key lengths for both symmetric and asymmetric encryption, such as triple DES and 1,024-bit RSA (SET 1997b). There is thus no risk of credit card numbers being compromised via interception. In addition, even if unauthorised access to a merchant web server occurs, the confidentiality of consumer payment information will not be endangered since it is encrypted using an acquiring bank public key. Thus SET can prevent credit card fraud arising from transmission and storage of sensitive data.

2.2 Merchant fraud

In SET, order and payment information are encrypted separately for specific recipients. That is, merchant public keys are used to encrypt order information and acquiring bank public keys are used to encrypt payment information. Consumers can thus be assured that their credit card numbers will not be compromised by a fraudulent merchant.

In addition, to prevent merchants modifying payment details, e.g. to increase the value of a sale, as part of SET the consumer PC adds a digital signature to all relevant transaction information.

2.3 Consumer fraud

Since the Internet offers no guarantees about the identity of the originator of a transaction, it is difficult for merchants to check whether consumers are using stolen credit card numbers to initiate transactions. In SET, consumers must authenticate themselves to their local PC by entering a password to activate their digital wallet prior to initiating a transaction. The consumer's PC then transmits completed order form and payment instructions to the merchant. As SET employs digital signatures to authenticate the cardholder PC, merchants can verify the legitimacy of the cardholder. This means that the SET scheme can address consumer fraud deriving from misuse of credit card numbers.

2.4 Internet fraud

The Internet link between customer and merchant may be subject to manipulation by a malicious third party. The use by SET of digital signatures, as mentioned in Section 2.2, prevents this.

3 ANALYSIS OF SET CRITICISMS

SET has been criticised for a variety of reasons, Hassler (2000), Gruman (1998), Lieb (1999), Treese and Stewart (1998). Some of the most significant criticisms are as follows.

- SET initialisation is complex. In particular, key pairs need to be established for each entity (and public keys certified).
- Interoperation of SET requires special software to be installed by every participating entity.
- SET is somewhat inflexible in that, since digital wallets need to be present in the consumer PC, performing e-commerce transactions from third party PCs (e.g. in airport lounges, Internet cafes, etc.) is difficult. There is a significant implementation cost for merchant and consumer.
- SET has not been widely adopted, and is widely perceived as being ‘dead’.
- The cryptographic complexity of SET makes it too slow for practical use, (Sherif 2000).

We now examine each of these criticisms in more detail.

3.1 The complexity of end-user initialisation

Unlike SSL, in which the use of digital certificates by end users is optional, every SET participant needs to obtain a key pair and a digital certificate for their public key, (Stein 1998). This adds considerable complexity to the initialisation process of SET for end-users (e-consumers). In more detail, a consumer needs to generate his/her own private-public key pair and then submit their identity with the public key to the issuing bank. This transfer needs to happen in a secure way, so that the bank knows that the public key has not been modified in transit and comes from the genuine account holder. The issuing bank then digitally signs the public key supplied by the account holder to create a digital certificate for the cardholder. The issuing bank must then distribute the certificate to the account holder. This process makes SET-based e-commerce initialisation complicated to conduct for both the consumer and the issuing bank. According to Lieb (1999, p. 2), “the effort to obtain digital certificates has held up deployment of SET technology”. This therefore appears to be one of the main reasons why SSL is almost always used in preference to SET for Internet e-commerce security. This is also supported by Treese and Stewart (1998) who argue that although SET cardholder certificates enable cardholder authentication, which reduces problems of fraudulent use of credit card numbers, this benefit causes more complexity and investment for the cardholder.

3.2 Interoperability

The use of SET relies on applications from several different software vendors and trusted third parties, such as Entrust Technologies, Globeset, Hitachi, IBM, and VeriSign. It is therefore crucial for these organisations to establish interoperable SET applications. For example, all major SET products, such as digital wallets, EFTPOS (Electronic Funds Transfer at Point of Sale) applications, payment gateway applications, and digital certificates, must work together. Problems with interoperability between different implementations has delayed the implementation of SET.

Nevertheless, a report on a SET software interoperability test conducted in 1999 (SET 1999c) indicates that interoperability problems are gradually being eliminated. This is because many SET products have now successfully passed interoperability tests provided by SETCo. By means of this testing regime, interoperability issues are gradually being resolved.

3.3 Flexibility

The e-commerce environment should be flexible for consumers, and enable them to place orders in a variety of locations including, for example, from homes, workplaces, or even Internet cafes. Since SET requires consumers to download a digital wallet to their computers, achieving this level of flexibility with SET is clearly problematic.

However, it could be argued that limiting flexibility is an acceptable price for security of financial information. Supporting this argument, the use of digital wallets has been extended to SSL as well as SET. It also seems that many software vendors are developing and standardising digital wallets in order to make it easier for consumers to use them. For example, the MasterCard wallet based on IBM wallet v2.1 (IBM 1999) supports both the SET and SSL protocols.

A recent paper by IBM states that consumers will in future be able to activate their digital wallets from any browser, and not just the default browser on their own device. This will be supported through the import and export of payment method information using portable secure devices including smart cards (IBM 1999). This will arguably make SET implementations significantly more flexible.

3.4 Cost of investment

Because the intention of SET is to secure the entire transaction process, special applications are required to implement SET (unlike SSL, which is built into commonly used web software). Hence the cost of implementation is another cause of concern for many e-commerce merchants, (Gruman 1998).

However, there are potential commercial advantages for merchants adopting SET rather than SSL. This is because, whilst the credit card payment system offers protection to cardholders in the event of fraud, this protection does not always extend to merchants. For example, merchants must bear the cost of ‘card not present’ chargebacks, (Caunter 2001), and e-commerce transactions protected using SSL are classified as ‘card not present’ transactions. By contrast, SET transactions are approved as ‘card present’ transactions (SET 1997a), and hence offer merchants protection against certain types of losses resulting from fraudulent use of cards. As a consequence, the cost to merchants of SET implementation can be offset against an anticipated reduction in costs associated with card fraud.

3.5 SET is dead

The fact that SET has been slow to gain acceptance has led many commentators to claim that SET is dead – this claim itself presents a barrier to wider acceptance of SET. However, SETCo reports that the number of SET users has risen over 300% since 1998. It is also claimed by SETCo that a number of merchants and financial institutions in US, Europe, Latin America and Asia are

currently using SET as a standard means for securing transactions. These statistics are not consistent with the idea that SET is defunct.

3.6 SET is too slow

The low speed and complexity of transactions is another commonly made criticism of SET that reduces its attractiveness to both merchants and consumers. It is sometimes stated that SET is very slow in comparison with other Internet e-commerce security protocols, such as SSL. This statement may be correct if we calculate the performance of SET when implemented using conventional techniques. However, according to a comparative performance analysis conducted by Gartner Group (1998), there are several implementation approaches that can be used to improve the performance of SET. These include cryptographic hardware acceleration, and elliptic curve cryptography. If these methods are applied to both SET and SSL, the performance of transactions is very similar.

4 PROSPECTS OF SET IMPLEMENTATION

In spite of the fact that SET would appear to be one of the most secure payment methods in e-commerce, significant hurdles still exist to its widespread adoption. Amongst the various difficulties SET presents, two of the most difficult to deal with are the need for the user information stored on a consumer PC to be protected, and the problems associated with initialisation. Since SET is based on the use of public key cryptography, there is also a risk of a private key being stolen from a consumer PC. In this section we consider how certain of the SET extensions may alleviate these problems.

4.1 PIN extensions

Whilst SET incorporates an element of password-based protection of the digital wallet at the consumer PC, the level of protection this offers might not be adequate to prevent unauthorised use of a credit card. Therefore it would be desirable to use the existing Personal Identification Number (PIN) associated with a payment card as an additional means of online cardholder authentication. This motivates the extension of the SET protocol to support the online transport of a cardholders' PIN.

In the SET online PIN extensions (SET 1999b), PINs are entered via a PC keyboard or a secure PIN entry device. As with a debit/credit card terminal in a merchant premises, cardholder applications must be able to verify which credit cards require PINs. In order that control can be exerted over the use of PINs, the SET payment gateway certificate can indicate the method of PIN entry permitted by the gateway, such as via a PC keyboard or a secure device. It is possible that, in some cases, the SET payment gateway certificate will state that no PIN entry methods are acceptable.

4.2 Chip extensions

As has already been mentioned, the fact that sensitive consumer payment information is stored in a PC and only protected by password authentication is a source of potential threats. In response to this issue, there are significant advantages to be gained from combining the SET protocol with a smart card (chip card, IC card or ICC) held by the user. If such a card can hold appropriate RSA keys and certificates, then the security issues associated with the digital wallet can be avoided. Since debit/credit IC cards conforming to the EMV (named after its inventors Europay, MasterCard, and Visa International) industry standard (EMV 2000a) and incorporating such keys are already being issued in large numbers, a major opportunity exists to use them to enhance SET security.

4.2.1 Overview of SET chip extensions

The chip extensions to SET version 1.0 (SET 1999a) enable SET to interoperate with IC cards conforming to the EMV industry standards. These extensions extend the SET protocol to support the transport of IC Card related data (EMV 1999).

In the EMV card authentication scheme, an issuer provides each IC card with its own private/public key pair. Each card will also contain a digital certificate for the card public key, signed by the issuer's private key. In addition, issuer public keys are certified by a brand Certification Authority (CA), set up by the owner of the card brand (e.g. Visa or MasterCard). The appropriate issuer public key certificate is then put on the card, along with the card public key certificate. In addition, the brand CA public keys are loaded into every merchant terminal. This then enables a merchant terminal to verify the pair of certificates held by the IC card, which then enables the merchant to verify the IC card's digital signature (EMV 2000b). This PKI structure is very similar to the PKI used by SET, and the SET chip extensions are designed to allow the EMV PKI to be exploited by SET without the need for SET-specific keys to be established at the cardholder. By means of these extensions the complexity of end-user initialisation when conducting SET can be eliminated, as there is no requirement for users to generate a key pair and apply for digital certificate. Figure 3 shows the combination of EMV dynamic authentication and SET, as specified in the chip extensions, (EMV 1999, SET 1999a).

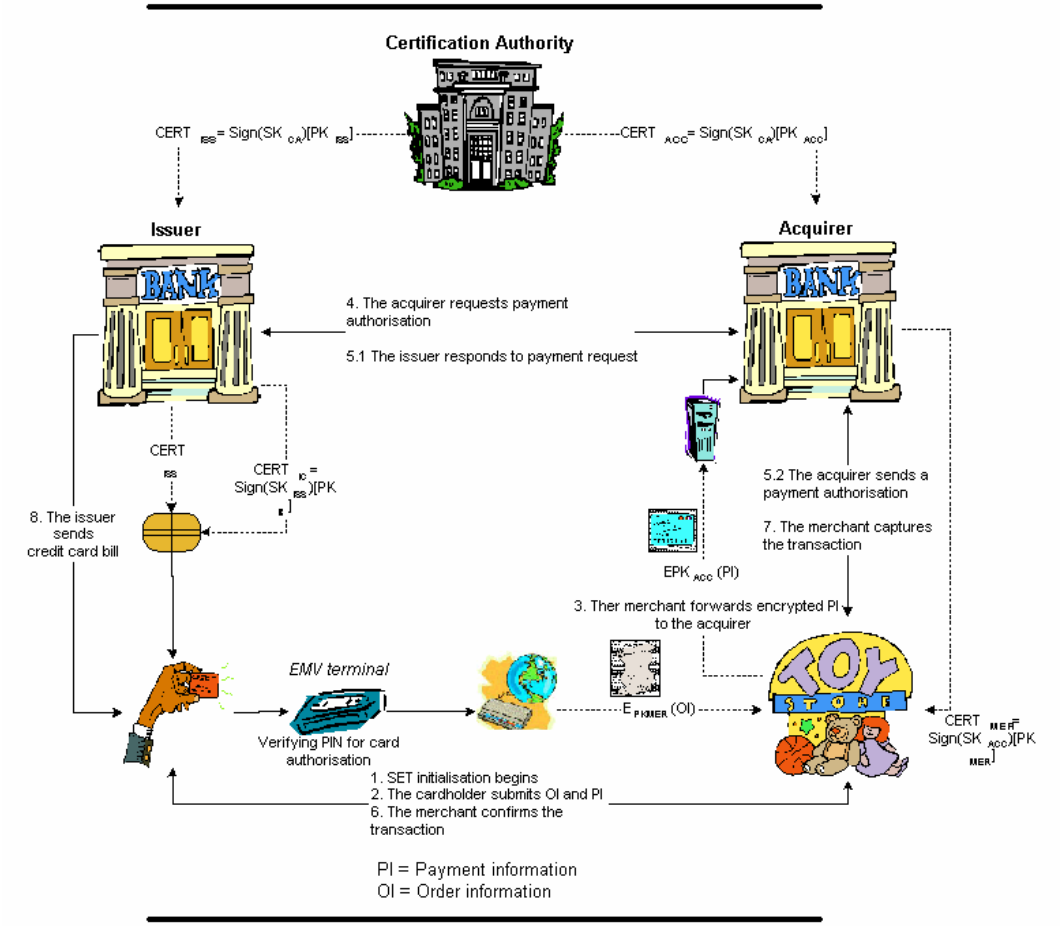

Figure 3. SET/EMV dynamic authentication in e-commerce transactions.

4.3 Analysis of the possibility of SET/EMV implementation

Conducting e-commerce with a combination of SET and EMV is currently a little complicated for consumers since it requires an additional device (an IC card reader) to be connected to the user PC.

However, a number of smart card manufacturers are attempting to facilitate the use of smart cards by PC owners.

Over and above the efforts of smart card manufacturers, the availability of appropriate smart card readers for consumer e-commerce is likely to be enhanced by the FINREAD (Financial transactional IC card reader) project. This project, part of the European Union IST (Information Society) programme, is designed to establish a secure smart card reader for use in consumer e-commerce, including home banking and Internet shopping. The FINREAD specifications (CWA 2001) provide a high level of security and are designed to support all forms of secure financial services transactions, including SET. Furthermore, in terms of compatibility/compliance with technical standards for IC cards, it is also claimed by FINREAD consortium that the FINREAD ICC reader *shall* be compatible with the EMV specifications. This provides further support for the future growth of EMV/SET as an e-commerce security solution.

FINREAD terminals are expected to be distributed from Europe to other countries and it is estimated that the market for readers may exceed 80 million units in Europe. Consumers will be able to purchase smart card readers at low costs without limiting the security and usability of the products (CWA 2001). Hence it is feasible that the IC card reader will become a widely adopted PC peripheral.

5 FUTURE OF SET IN E-COMMERCE

From the above analysis of SET criticisms and the use of SET extensions, it would appear that the SET system still has a potentially important role to play in securing e-commerce transactions. Consumers, merchants, and financial institutions all benefit from the protection of the secure environment offered by the SET protocol. The combination of SET and EMV chip cards will be particularly beneficial since it addresses both the digital wallet security issues and the complexity of end-user initialisation. As a result, the conclusions of this study of the future of SET can be summarised as below.

- Whilst SET has been slow to take off, one of the main hurdles to its adoption, namely the cost and complexity of initialisation, can be significantly reduced through the use of the chip extensions.
- SET interoperability issues are being solved through the use of interoperability testing software produced by SETCo.
- SET flexibility issues are being addressed in a variety of ways, including the development of portable digital wallets.
- The cost of investment to merchants can be offset against reduced fraud costs.
- SET is not dead, as is often stated – indeed SET is still being developed.
- The speed of SET is comparable of that of other security techniques, given that it is implemented in appropriate ways.

6 CONCLUSION

SET is arguably the only currently available scheme for providing security for entire e-commerce transactions. Although there are many criticisms of SET, we have shown that all these criticisms can be addressed, and that SET still has the potential to overcome the barriers that restrict its implementation. In particular the various extensions to SET seem to both enhance its security and reduce the complexity of SET implementation. Hence we believe that the SET secure transactions method has the potential to be widely used not only in Internet e-commerce security but also in other methods of payment where the potential for fraud is of particular concern to the e-consumer.

Although SSL is almost always used in preference to SET for Internet e-commerce security at present, implementation of SET in e-commerce may be just a matter of time. Given potential e-commerce participants are very concerned about the threat of credit card fraud, cooperation between public and private sectors would seem to be a possible enabler for the future adoption of this alternative scheme. One way in which the adoption of SET could be facilitated would be if governments or trade bodies positively encouraged merchants and card issuers to adopt SET, e.g. by requiring its use for their e-business. However, for such a move to become reality would require a positive decision in favour of SET by official bodies, which seems to be some way from reality in the current climate.

References

Caldwell, K. (2000). **Global electronic commerce – moving forward**. *CommerceNet: The Public Policy Report*, 2(11): 2-17.

Caunter, N. (2001). **The real cost of fraud to e-tailers**. *Computer Fraud and Security*, 2001(8): 17.

EMV (1999). *EMV '96 Chip Electronic Commerce Specification*. EMVCo.Org. Version 1.0.

EMV (2000a). *EMV 2000 Integrated Circuit Card Specification for Payment Systems – Book 1: Application Independent ICC to Terminal Interface Requirements*. EMVCo.Org. Version 4.0.

EMV (2000b). *EMV 2000 Integrated Circuit Card Specification for Payment Systems – Book 2: Security and Key Management*. EMVCo.Org. Version 4.0.

CWA (2001). *CWA 14174-1 Financial transaction IC card reader (FINREAD) – Part 1: Business requirements.*

Gartner Group (1998). *SET Comparative Performance Analysis*. Gartner Group.

Gruman, G. (1998). *E-commerce not ready for SET*. Computer World.
Available from http://www.computerworld.com/cwi/story/0,1199,NAV47_STO31581,00.html
(last accessed November 30, 2001).

Hassler, V. (2000). *Security Fundamentals for E-Commerce*. Artech House. Massachusetts.

IBM (1999). *Internet Wallet Choices and Answers for Business and Technical Managers*. IBM e-business.

Lieb, J. (1999). **Getting secure online – an overview**, *CommerceNet – The Strategies Report*, 1(3): 1-4, July.

Sherif, M. H. (2000). *Protocols for Secure Electronic Commerce*. CRC Press. Florida.

Oppliger, R. (2000). *Security Technologies for the World Wide Web*. Artech House. Massachusetts.

Rescorla, E. (2001). *SSL and TLS – Designing and Building Secure Systems*. Addison-Wesley. Boston.

SET (1997a). *SET Secure Electronic Transaction Specification – Book 1: Business Description*. SETCo.Org. Version 1.0.

SET (1997b). *SET Secure Electronic Transaction Specification – Book 2: Programmer's Guide*. SETCo.Org. Version 1.0.

SET (1999a). *Common Chip Extension – Application for SETCo Approval*. SETCo.Org. Version 1.0.

SET (1999b). *Online PIN Extensions to SET Secure Electronic Transaction*. SETCo.Org. Version 1.0.

SET (1999c). *SET Secure Electronic Transaction LLC – Interoperability Festival Results*. SETCo.Org.

Stein, L. D. (1998). *Web Security*. Addison-Wesley. Boston.

Treese, G. W. and Stewart, L. C. (1998). *Designing Systems for Internet Commerce*. Addison-Wesley. Massachusetts.

Whiteley, D. (2000). *E-Commerce: Strategy, Technologies and Applications*. McGraw-Hill. Berkeley.